| **Data Source** | **Type** | **Why Useful** | **Small Description** | **Download Sources** | **Update Frequency** |
| --- | --- | --- | --- | --- | --- |
| **MITRE ATT&CK** | Knowledge Base of Adversary Tactics & Techniques | Standardized mapping of attacker behaviors to real-world techniques, essential for correlation and detection logic | Detailed framework of known adversary tactics, techniques, and procedures (TTPs) mapped to intrusion stages | <https://attack.mitre.org/> (STIX/TAXII feeds) | Updated multiple times per year |
| **ExploitDB** | Public Exploit & PoC Database | Quickly links vulnerabilities to publicly available exploits, useful for prioritizing remediation | Archive of public exploits, PoCs, and related shellcode | <https://www.exploit-db.com/> (CSV dumps, search API) | Daily updates |
| **CISA KEV** | Known Exploited Vulnerabilities List | Helps prioritize patching based on actively exploited vulnerabilities | US-CERT-maintained list of vulnerabilities known to be actively exploited in the wild | <https://www.cisa.gov/known-exploited-vulnerabilities-catalog> (JSON/CSV feeds) | Daily to weekly updates |
| **Sigma Rule Repository** | Detection Rules (Generic SIEM Queries) | Provides generic detection rules that can be converted to multiple SIEM platforms | Open repository of detection rules written in Sigma syntax | <https://github.com/SigmaHQ/sigma> (GitHub repo clone) | Updated frequently, often daily |
| **YARA Rule Repos** | Malware Detection Signatures | Detects and classifies malware in files, memory, or network traffic | Ruleset-based detection for specific malware families or behaviors | Multiple: e.g., <https://github.com/Yara-Rules/rules> | Updated daily to weekly depending on source |
| **MalwareBazaar / VirusTotal / AnyRun** | Malware Samples & Analysis | Provides real-world malware binaries, hashes, and sandbox analysis reports | MalwareBazaar: community-driven malware repository; VirusTotal: multi-engine malware scan & metadata; AnyRun: interactive malware sandbox | MalwareBazaar: <https://bazaar.abuse.ch/> (API); VirusTotal: <https://www.virustotal.com/> (API key required); AnyRun: <https://any.run/> | Near real-time updates |
| **Security Incident Datasets (CERT, APT Notes)** | Incident Reports & Threat Actor Analysis | Provide historical attack patterns and actor profiles for training models | Incident reports from CERT teams, APT group activity writeups, forensic data | CERT: <https://www.cert.org/>; APT notes: <https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections> | Varies by incident occurrence |
| **Open Threat Exchange (OTX)** | Threat Intelligence Sharing Platform | Community-contributed IoCs, useful for real-time threat detection | AlienVault's collaborative threat intel platform where researchers share IoCs | <https://otx.alienvault.com/> (API) | Near real-time updates |

| **Datasource** | **Type** | **Why Useful** | **Small Description** | **Download Sources** | **Update Frequency** |
| --- | --- | --- | --- | --- | --- |
| **MITRE D3FEND** | Defensive techniques knowledge base | Maps to ATT&CK but from a defensive lens; helps in building mitigation strategies | A framework of cybersecurity countermeasures linked to ATT&CK tactics/techniques | [https://d3fend.mitre.org](https://d3fend.mitre.org/) | Irregular (when updated by MITRE) |
| **CAPEC** (Common Attack Pattern Enumeration) | Attack pattern database | Useful for understanding how attacks work at a pattern level | Public catalog of common attack patterns and their relationships to vulnerabilities | <https://capec.mitre.org/data/downloads/> | Few times/year |
| **VulnCheck** | Vulnerability intelligence | Provides enriched vulnerability context beyond NVD | Commercial source that correlates vulnerabilities with exploits, malware, and threat actors | [https://vulncheck.com](https://vulncheck.com/) | Daily |
| **VulDB** | Vulnerability database | Gives extra details on CVEs, sometimes earlier than NVD | Public/commercial vulnerability intelligence portal with extra metadata | [https://vuldb.com](https://vuldb.com/) | Daily |
| **Snyk Vulnerability DB** | Open source & dependency vulnerability database | Helps developers identify security issues in dependencies | Security database focusing on open source packages, with developer-friendly details | [https://security.snyk.io](https://security.snyk.io/) | Daily |
| **Snort/Suricata Rules** | IDS/IPS detection rules | Enables network-based detection of threats | Rule sets for detecting malicious traffic patterns | <https://www.snort.org/downloads> / <https://suricata.io/rules/> | Daily/Weekly |
| **Elastic Detection Rules** | SIEM detection rules | Prebuilt correlation and detection content for Elastic Security | Repository of Sigma-like rules for Elastic SIEM | <https://github.com/elastic/detection-rules> | Weekly |
| **Splunk Security Content** | SIEM detection content | Prebuilt searches and analytics for threat detection in Splunk | Detection logic, playbooks, and analytics for Splunk Enterprise Security | [https://research.splunk.com](https://research.splunk.com/) | Weekly |
| **VX Underground** | Malware repository | Access to malware samples for research/testing | One of the largest malware sample archives | [https://vx-underground.org](https://vx-underground.org/) | Daily |
| **AlienVault OTX** (Open Threat Exchange) | Threat intelligence sharing | Crowdsourced IOCs and threat reports | Public platform for exchanging threat data | [https://otx.alienvault.com](https://otx.alienvault.com/) | Daily |
| **MISP Threat Sharing** | Threat intelligence sharing platform | Standardized sharing of threat indicators | Open source threat intelligence sharing platform | <https://www.misp-project.org/download/> | Continuous (depends on feed) |
| **ThreatFox** (Abuse.ch) | IOC feed | Real-time IOC feed for active threats | Collection of malicious indicators shared by community | <https://threatfox.abuse.ch/downloads/> | Hourly/Daily |
| **PhishTank** | Phishing URL database | Helps detect and block phishing sites | Community-driven list of verified phishing sites | <https://phishtank.org/developer_info.php> | Daily |
| **URLhaus** (Abuse.ch) | Malicious URL feed | Focused on malware delivery URLs | Community-driven malware URL database | <https://urlhaus.abuse.ch/downloads/> | Hourly/Daily |

| **Datasource** | **Type** | **Why Useful** | **Small Description** | **Download Sources** | **Update Frequency** |
| --- | --- | --- | --- | --- | --- |
| **Feodo Tracker (Abuse.ch)** | Botnet C2 Tracker | Identifies and tracks known botnet Command & Control servers | Provides blocklists of IPs/domains associated with malware like TrickBot, QakBot, Dridex | [https://feodotracker.abuse.ch](https://feodotracker.abuse.ch/) | Daily / Multiple times a day |
| **CyberGreen** | Internet Health Metrics | Measures & reports on global cybersecurity hygiene | Aggregates data on insecure services, vulnerabilities, and misconfigurations globally | <https://www.cybergreen.net/data> | Monthly / Quarterly |
| **MITRE Engenuity ATT&CK Evaluations** | Security Product Evaluation | Helps evaluate EDR/XDR tools against ATT&CK techniques | Simulates APT attack scenarios and measures how well products detect/respond | <https://attackevals.mitre-engenuity.org/> | Annually |
| **CERT Reports (US-CERT, etc.)** | Security Incident & Advisory Reports | Provides authoritative advisories and mitigations | Detailed technical reports on vulnerabilities, incidents, and attack campaigns | <https://www.cisa.gov/uscert/ncas> | Weekly / As needed |
| **Mandiant Reports** | Threat Intelligence Reports | Deep analysis of advanced persistent threats (APTs) | Insights into attacker TTPs, campaigns, and malware from real-world incidents | <https://www.mandiant.com/resources> | Monthly / Incident-driven |
| **Kaspersky Threat Intelligence** | Threat Intel Platform | Commercial-grade threat data feeds | IOC feeds, malware analysis, APT tracking, and vulnerability intelligence | <https://www.kaspersky.com/enterprise-security/threat-intelligence> | Daily |
| **DarkNet Scan Feeds** | Dark Web Monitoring | Early warning for leaked data & underground chatter | Crawls hidden services for stolen credentials, exploits, and trade chatter | Vendor-specific (commercial) | Daily |
| **DDoSecrets** | Leaked Data Repository | Access to datasets from leaks & breaches | Nonprofit publishing data from hacks, leaks, and breaches for research | [https://ddosecrets.com](https://ddosecrets.com/) | Irregular / As obtained |
| **GreyNoise** | Internet Background Noise Analysis | Filters out benign internet scanning from malicious activity | Provides context on IPs scanning the internet and their intent | [https://viz.greynoise.io](https://viz.greynoise.io/) | Daily |
| **Shodan** | Internet Asset Search Engine | Finds internet-connected devices & vulnerabilities | Indexes IoT devices, servers, and open services with metadata & vulnerabilities | [https://www.shodan.io](https://www.shodan.io/) | Continuous |
| **Censys** | Internet Exposure Mapping | Tracks internet-facing assets for security posture | Monitors certificates, services, and configurations for risk | [https://search.censys.io](https://search.censys.io/) | Continuous |
| **RiskIQ Community Edition** | Threat Intelligence Platform | Maps attacker infrastructure | Tracks domains, IPs, SSL certs, and WHOIS data for threat hunting | [https://community.riskiq.com](https://community.riskiq.com/) | Daily |